The request specifies the identity whose data is desired to be operated upon, as well as the type of document that is desired to he accessed (e.g., content, role list, system). Based on this, the authorization station may identify the appropriate role list. The authorization station selects the appropriate role definition within the role list using the user identifier, the application identifier, and the platform identifier specified in the request. Also, the type of credentials used to authenticate are also used to identify the appropriate role definition. Thus, one user using a more secure authentication mechanism may be granted more extensive access than the same user with the same application but using a less secure authentication mechanism.

When the authorization station receives a request from the requesting entity to perform at least one of the command methods, the authorization station then identifies the appropriate role definition. Using this role definition, the authorization station determines access permissions for the requesting entity with respect to the requested action.

The present invention has the advantage of performing authorization in a standardized manner regardless of the target service that is desired. The service is only factored in when selecting an appropriate role map. In addition, this is accomplished while providing a standardized set of templates that may be used for coarse-grained control over access. Thus, applications that are not able to add further refined scopes to the role list may at least have some level of access control over the service's data structures. In addition, those that can define more refined scopes may have those more refined scopes included in the role list documents to allow for more user-specific and refined control over access permissions. These refined scopes may be included in the role list corresponding to the identity whose data is being accessed. Accordingly, the present invention provides for a high level of control over access permissions in a manner that is relatively independent of the underlying service being targeted.

Additional features and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of the invention. The features and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to describe the manner in which the above-recited and other advantages and features of the invention can be obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

FIG. **1** schematically illustrates a general network environment in which the present invention may be employed;

FIG. **2** illustrates a specific example of a network environment in which the present invention may be employed;

FIG. **3** illustrates data structures including a role list data structure linked by reference with a role map data structure, the data structures being used to authorize a requestor to perform certain actions on identified data structures;

FIG. **4** illustrates a flowchart of a method for authorizing a requestor to perform certain actions on the identified data structure; and

FIG. **5** schematically illustrates a computing device that may implement the features of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention extends to methods, systems and computer program products for authorizing a requesting entity in a manner that is at least partially independent of the underlying target data structure that is desired to be accessed. In one operating environment, there are a number of individuals and applications operating through a variety of services on a variety of different types of identity-specific data structures that are organized in accordance with a set of rules. Each service is configured to perform operations on one or more different types of data structures. For example, an identity may have an in-box data structure organized in accordance with an in-box schema and that is managed by an in-box service, a calendar data structure organized in accordance with a calendar schema and that is managed by a calendar service, and so forth.

The principles of the present invention allow for authorization of a requesting entity to occur largely, if not wholly, independent of the type of the underlying data structure that is desired to be operated upon. This allows for a centralized authorization station that performs the entire authorization process for a wide variety of different services. The centralized authorization station may then inform the target service that the requested operation is authorized and provide the service with sufficient information to perform the desired operation on the target data structure.

Embodiments within the scope of the present invention may comprise a special purpose or general purpose computing device including various computer hardware, as discussed in greater detail below. Embodiments within the scope of the present invention also include computer-readable media for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media which can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise physical storage media such as RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer.

When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions.